

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 2:16cr95
)	
ROBERT MCLAMB)	

DEFENDANT’S SECOND MOTION TO SUPPRESS

Robert McLamb, through counsel and pursuant to Federal Rule of Criminal Procedure 12(b)(3)(c), respectfully moves this Court for an order suppressing all evidence seized from Mr. McLamb’s home computer by the FBI on or about February 28, 2015 through the use of a network investigative technique (“NIT”), as well as all fruits of that search. The NIT Warrant that purported to authorize this search was void *ab initio* and therefore the warrantless search was unconstitutional. Mr. McLamb also alleges a prejudicial and deliberate violation of Rule 41, which independently warrants suppression. An evidentiary hearing is requested.

INTRODUCTION

As the Court is aware from Defendant’s First Motion to Suppress, all of the government’s evidence in this case can be traced back to its remote search of Mr. McLamb’s home computer through the use of NIT malware. This search was purportedly authorized by the February 20, 2015 “NIT Warrant” issued by Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. *See* Ex. A.¹ Because neither the Federal Magistrates Act nor Rule 41(b) authorized the magistrate judge to issue it, the NIT Warrant—issued without lawful authority—was void *ab initio*. A warrant void from its inception is no warrant at all. The

¹ Throughout this Motion, the defense cites to Exhibits attached to Defendant’s First Motion to Suppress since the factual background for both are the same.

government's search here was thus warrantless and violated the Fourth Amendment. Alternatively, the Court could avoid reaching the constitutional question and grant suppression after finding a deliberate violation of Rule 41(b) that prejudiced Mr. McLamb. In either case, suppression is warranted.

STATEMENT OF FACTS

Mr. McLamb incorporates here the statement of facts from his First Motion to Suppress. To summarize, however, the basic facts are as follows:

In February 2015, the government physically seized a server from which an individual in Florida had been operating a website on the "Tor" network. This website is referred to in various government documents as "Website A" or the "Target Website" but it is commonly known as "Playpen." The FBI moved the Playpen server to a location in the Eastern District of Virginia and continued to operate the Playpen website for about a month.

Right after seizing the server, the government applied for a search warrant that would authorize it to install NIT malware on the computer of anyone who clicked through Playpen's homepage. Because the site was operated on the Tor network, the government could not identify the physical location of accessing computers without searching each computer first through the use of its NIT malware.

The government submitted a warrant application to a federal magistrate judge in the Eastern District of Virginia. (As discussed in the Defendant's First Motion to Suppress, the defense maintains that the warrant application contained many inaccuracies and did not make a probable cause showing sufficient to support the broad searching authority that it sought—but those questions are not at issue here.) The magistrate signed the warrant, which identified all "activating computers" as the places to be searched. Ex. A, 2. The warrant clarified that

“activating computers” are the computers “of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.” Ex. A, 2.

It is undisputed that the FBI did not know and could not have known the physical location of any “activating computer” before it searched that computer through the deployment of its NIT malware.

On or about February 28, 2015, FBI agents sent the NIT malware to a user’s computer and seized data from it. The FBI used data they seized from this computer to determine its physical address: Mr. McLamb’s home in Virginia Beach, Virginia. On December 1, 2015, the government obtained a traditional residential search warrant—based on the information it obtained through the NIT search—which authorized the search of Mr. McLamb’s home. Pursuant to that warrant agents seized a large amount of electronic equipment, including a Xion desktop computer and two hard disk drives on December 8, 2015. In sum, all of the government’s evidence traces directly back to the malware search it conducted pursuant to the NIT Warrant issued by Magistrate Judge Buchanan.

LAW & ARGUMENT

Within the last few months, two federal courts have granted suppression motions finding that the NIT Warrant—which purported to authorize the FBI’s search of Mr. McLamb’s computer and countless others across the country²—was void *ab initio* because the magistrate judge lacked any legal authority to issue it. United States District Judge William G. Young summarized:

² See Joseph Cox, *The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a Thousand Computers*, Motherboard (Jan. 5, 2015), available at <http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers> (last visited Apr. 29, 2016).

[T]he Court concludes that the NIT Warrant was issued without jurisdiction and thus was void *ab initio*. It follows that the resulting search was conducted as though there were no warrant at all. Since warrantless searches are presumptively unreasonable, and the good-faith exception is inapplicable, the evidence must be excluded.

United States v. Levin, Crim. No. 15-10271, --- F.Supp.3d ---, 2016 WL 2596010, at *15 (D. Mass. May 5, 2016); *see also United States v. Arterbury*, Crim. No. 15-182, ECF No. 47 (N. D. Okla. May 12, 2016) adopting Report and Recommendation, ECF No. 42 (“The NIT Warrant clearly did not comport with Fed. R. Crim. P. 41(b), and, therefore, was invalid *ab initio*.”). As the *Levin* court concluded, “neither the Federal Magistrates Act nor Rule 41(b) authorized the issuance of the NIT Warrant.” *Levin*, at *7. “[A] warrant issued in defiance of positive law’s jurisdictional limitations on a magistrate judge’s powers” is “no warrant at all.” *United States v. Krueger*, 809 F.3d 1109, 1126 (10th Cir. 2015) (Gorsuch, J., concurring). Accordingly, all fruit of the government’s warrantless search in this case must be suppressed.

A. Under the Federal Magistrates Act, a Magistrate Judge Lacked Jurisdiction to Issue the NIT Warrant.

“Section 636(a) of the Federal Magistrates Act establishes ‘*jurisdictional* limitations on the power of magistrate judges.’” *Levin*, at *3 (quoting *Krueger*, 809 F.3d at 1122 (Gorsuch, J., concurring)). *Cf. United States v. Bryson*, 981 F.2d 720, 726 (4th Cir. 1992) (vacating magistrate judge’s order because magistrate exceeded jurisdictional limitations imposed by Federal Magistrates Act). The Federal Magistrates Act limits the authority of a magistrate judge so that he or she may exercise the powers and duties conferred by the Federal Rules of Criminal Procedure only “within the district in which sessions are held by the court that appointed the magistrate judge,” “at other places” where her court may function, or “elsewhere” as authorized by some other law. 28 U.S.C. § 636(a). Here, without having to look beyond the first paragraph of § 636, it is clear that the magistrate purported to exercise power conveyed by the Federal

Rules—*i.e.*, the power to issue a search warrant—but she exercised that power over places that met none of § 636(a)’s self-contained geographic criteria. *See Krueger*, 809 F.3d at 1119 (Gorsuch, J., concurring). This is enough to brand the warrant unauthorized.

But in any event, the *Levin* court correctly held that “[f]or the magistrate judge to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41(b).” *Levin*, at *8 n.11. This is because no other jurisdictional grant in subsections (2) through (5) of § 636(a) is applicable. And no other law or Rule of Criminal Procedure provides a magistrate—through § 636(a)(1)—the jurisdiction to authorize nationwide searches. As discussed below, the territorially unrestricted NIT Warrant was not authorized by Federal Rule of Criminal Procedure 41(b).

Critical to the analysis here is the following: Because § 636(a) explicitly limits the *jurisdiction* of magistrate judges by reference to the Federal Rules of Criminal Procedure, a finding that the magistrate judge acted beyond her authority under Rule 41(b) means that she acted *beyond her jurisdiction* under § 636(a). As discussed in more detail below, the issuance of a warrant without statutory authority means that the NIT Warrant was *void at the time it was issued*. The constitutional implications of this conclusion are self-evident.

B. The NIT Warrant Was Not Authorized by Rule 41.

The NIT Warrant ignored the clearly established jurisdictional limits set forth in Federal Rule of Criminal Procedure 41. It allowed FBI agents to conduct a borderless dragnet search with *no geographic limitation*. Rule 41 simply does not permit a magistrate judge to authorize the searches of computers around the country or around the world.

Rule 41(b) provides a magistrate judge with authority to issue a warrant in five unambiguous circumstances:

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- *has authority to issue a warrant to search for and seize a person or property located within the district*;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41 (emphasis added). The warrant in this case was not authorized under any of these sections and is therefore plainly unlawful.

1. The NIT Warrant is Not Authorized Under Rule 41(b)(1).

Rule 41(b)(1) allows a magistrate judge to issue a warrant for people or property located within that judge's district. Under the NIT Warrant the "place to be searched" was the myriad of "activating computers — *wherever located*" that would unknowingly download the NIT, thereby forcing the transmission of their internal data back to the FBI. Ex. B, ¶ 46 (emphasis added); *see also* Ex. A (noting that the NIT would be deployed to obtain information from "activating computers" and defining "activating computers" as "those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password"). The NIT Warrant authorized these searches even though there was no basis from which to conclude that these computers would be located in the Eastern District of Virginia. In fact, there was no way the FBI could tell—until *after* they conducted their search—in which judicial district the property they just searched was located. *See* Ex. B, ¶ 34 (explaining that purpose of searching user's computer was to "assist in identifying the user's computer, [and] its location").

Indeed, pursuant to the NIT Warrant the government searched computers located in Washington, Massachusetts, Ohio, Oklahoma, and the list goes on. It appears that the FBI searched computers in at least 18 different judicial districts. *See* Gabrielle Banks, *Federal agents sweep child pornography site by hacking 'dark web' site*, Houston Chron. (Apr. 10, 2016) (reporting that warrant at issue here has "led to the arrest of more than 135 people in 18 states on child pornography charges"). As the *Levin* court held, "That the Website A server is located in the Eastern District of Virginia is, for purposes of Rule 41(b)(1), immaterial, since it is not the server itself from which the relevant information was sought." *Levin*, at *5. The critical fact is

that “at least some of the activating computers [searched by the use of NIT malware] were located outside of the Eastern District of Virginia.” *Id.*

Rule 41(b)(1) cannot be the basis for dragnet searches with *no territorial restriction*.

2. No Other Subsection of Rule 41(b) Authorized the NIT Warrant.

The other subsections of Rule 41(b) are inapplicable to this case. Rule 41(b)(2) allows an extraterritorial search or seizure of moveable property if it is located within the district when the warrant is issued but might move or be moved before the warrant is executed. Here there was no evidence in the warrant application that all activating computers were located in the Eastern District of Virginia at the time the warrant issued. Indeed, they were not. The government did not and by its own admission could not say where the activating computers were or where they had been. In other cases, the government has argued that because the NIT (*i.e.*, the computer code used to generate the identifying information from users’ computers) was located in the Eastern District of Virginia at the time the warrant was issued, this subsection applies. But courts have rejected this argument. Because “the actual property to be searched was not the NIT nor the server on which it was located, but rather the users’ computers Rule 41(b)(2) is inapposite.” *Levin*, at *6.

It is also important to recognize that Rule 41(b)(2) “does not authorize a warrant in the converse situation—that is, for property *outside* the district when the warrant is issued, but brought back *inside* the district before the warrant is executed.” *In re Warrant*, 958 F. Supp. 2d at 757 (S.D. Tex. 2013). Thus, it is inapposite that the government planned to collect the data that it seized from activating computers around the world and ultimately store that data in the Eastern District of Virginia. If this were the standard, a) the text of Rule 41 would say so, and b) “there would effectively be no territorial limit for warrants involving personal property, because

such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.” *Id.*

Likewise, Rule 41(b)(3) cannot serve as a basis because this case does not involve terrorism.

Rule 41(b)(4) allows for tracking devices to be installed within the issuing district on an object that may travel to outside the district. The NIT here was installed activating computers without any assurance that these computers were (or ever had been) physically located within the Eastern District of Virginia for any “tracking device” to be installed. Although the government has argued in other NIT cases that Rule 41(b)(4) authorizes these searches, that argument has been consistently rejected. *See, e.g., Levin*, at *6 (rejecting argument); *United States v. Michaud*, Crim. No. 3:15- 05351, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016) (same); *In re Warrant*, 958 F.Supp.2d at 758 (same, noting that “there is no showing that the installation of the ‘tracking device’ (*i.e.* the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.”).

Rule 41(b)(5) does not apply to the NIT Warrant because there was no showing that all activating computers (or any for that matter) were located within any of the locations covered by this subsection.

No portion of Rule 41(b) authorized the nationwide searches contemplated by the NIT Warrant.

C. Suppression is Warranted.

“There are two categories of Rule 41 violations: those involving constitutional violations, and all others.” *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000). Here, issuance of

the NIT Warrant exceeded the territorial limitations of Rule 41(b), meaning it was issued without legal authority under § 636(a), which violates the Fourth Amendment.

But even if the Court finds that the Rule 41 violation does not rise to a constitutional level, the Rule 41 violation is substantive—not merely technical—and Mr. McLamb was prejudiced by the violation. Moreover, the government intentionally violated Rule 41 by requesting a warrant that was clearly outside the magistrate’s legal authority. For these reasons, suppression is warranted.

1. Because the NIT Warrant Was Issued Without Legal Authority, It Was Void From Its Inception and the Resulting Warrantless Search Requires Suppression under the Fourth Amendment.

Through § 636(a) and Rule 41(b), federal law designates those individuals who qualify as ‘neutral and detached magistrates’ and defines their jurisdictional authority to issue warrants under the Fourth Amendment. *See United States v. Master*, 614 F.3d 236, 241 (6th Cir. 2010). Unlike more procedural aspects of the Rules, “Section 636(a)’s territorial restrictions are *jurisdictional* limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation—quite unlike the violation of a more prosaic rule or statute—is *per se* harmful.” *Krueger*, 809 F.3d at 1122 (Gorsuch, J., concurring) (citing *Torres v. Oakland Scavenger Co.*, 487 U.S. 312, 317 n.3 (1988)). And as discussed above, the NIT Warrant exceeded the relevant jurisdictional limitations. Thus, the issuing magistrate judge lacked legal authority to issue the NIT Warrant in the first place.

The question then turns to what significance that has under the Fourth Amendment. In short: a lot.

[L]ooking to the common law at the time of the framing it becomes quickly obvious that a warrant issued for a search or seizure beyond the territorial jurisdiction of a magistrate’s powers under positive law was treated as no warrant at all—as *ultra vires* and *void ab initio* to use some of the law’s favorite Latin phrases....

So, for example, a justice of the king's bench with nationwide territorial jurisdiction afforded by Parliament could issue a warrant anywhere in the kingdom. Meanwhile, warrants issued by justices of the peace—county officials empowered to act only within their respective counties—were executable only within those same limited bounds. *See, e.g.*, 4 William Blackstone, Commentaries *291–92; 2 Matthew Hale, *Historia Placitorum Coronae* 111 (1736); *Engleman v. Deputy Murray*, 546 F.3d 944, 948–49 (8th Cir. 2008).... The principle animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official.

Krueger, 809 F.3d at 1123–24 (Gorsuch, J., concurring) (footnotes omitted). More recent cases follow this historical tradition. For example, in a recent series of cases, the Sixth Circuit has explained that the positive law—in these cases, state law—that defines the authority of the warrant issuer is constitutionally significant under the Fourth Amendment.

In *United States v. Master*, the defendant sought to suppress evidence obtained through a state search warrant. 614 F.3d 236, 239 (6th Cir. 2010). It was uncontested that the authorizing judge “did not have jurisdiction under Tennessee law to authorize a warrant for property in a different county,” yet that is what the warrant purported to authorize. *Id.* Thus the Sixth Circuit had to decide whether the lack of authority under state statutory law caused a violation of the federal constitution. The court held that it did. *Id.*

The government in *Master* argued that additional protections a state provides its citizens against search and seizure are irrelevant in federal prosecutions. But the Sixth Circuit noted that the warrant was not invalid because of additional protections provided by the state. “Instead, the warrant is invalid because it does not comply with the Fourth Amendment.” *Id.* The court held that “[t]he jurisdictional limits placed on [the state judge] are not additional protections for a citizen but instead merely a reflection of the authority vested by the state in a general sessions judge.” *Id.* The *Master* court then cited its decision in *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001), where the court held, “when a warrant is signed by someone who lacks the legal

authority necessary to issue search warrants, the warrant is void *ab initio*.” *Id.* (quotation from *Scott*).

The Sixth Circuit held that the Fourth Amendment’s warrant requirement incorporates the positive law’s rules about who is authorized to issue warrants and under what circumstances. *Master*, 614 F.3d at 240-41. In *Master*, Tennessee law provided that a magistrate’s jurisdiction was limited to issuing search warrants for property located within his county. Thus, the Sixth Circuit held, the state court judge “simply did not have the authority to issue a warrant to search a property in Coffee County.” *Id.* Critically, because the magistrate acted outside the jurisdiction set by the positive law of the relevant sovereign, this lack of state statutory authority created a problem under the Fourth Amendment of the Constitution of the United States. *Id.*

The Fourth Amendment demands a “valid warrant,” and for warrants to be valid they must emanate from “magistrates empowered to issue” them. *United States v. Lefkowitz*, 285 U.S. 452, 464 (1932). “Time and again state and circuit courts have explained that this means a warrant issued in defiance of positive law’s restrictions on the territorial reach of the issuing authority will not qualify as a warrant for Fourth Amendment purposes.” *Krueger*, 809 F.3d at 1124 (Gorsuch, J., concurring) (citing *State v. Kirkland*, 442 S.E.2d 491, 491-92 (Ga. App. 1994); *State v. Jacob*, 924 N.E.2d 410, 415-16 (Ohio App. 2009); *Sanchez v. State*, 365 S.W.3d 681, 684–86 (Tex. Crim. App. 2012); *Weinberg v. United States*, 126 F.2d 1004, 1006-07 (2d Cir. 1942); see also *United States v. Baker*, 894 F.2d 1144 (10th Cir.1990) (per curiam); *United States v. Barber*, Crim. No. 15-40043, 2016 WL 1660534, at *3 (D. Kan. Apr. 27, 2016) (noting that “[c]ourts have found that warrants issued without jurisdiction are void from their inception” and collecting cases).

To be sure, Rule 41 contains “both procedural and substantive provisions.” *Levin*, at *7. And violations of Rule 41’s “ministerial or technical” procedural requirements have generally been deemed not to warrant suppression. *Id.* But “this case involves a violation of Rule 41(b), which is a substantive provision.” *Id.* (quoting *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008)); *see also Krueger*, 809 F.3d at 1115 n.7 (noting that Rule 41(b)(1) “is unique from other provisions of Rule 41 because it implicates ‘substantive judicial authority,’” and concluding that cases involving violations of other subsections of Rule 41 “offer limited guidance”).³ What is more, the lack of compliance with Rule 41(b)’s substantive territorial restrictions means,

the NIT Warrant was issued without jurisdiction and thus was void *ab initio*. It follows that the resulting search was conducted as though there were no warrant at all. Since warrantless searches are presumptively unreasonable...the evidence must be excluded.

Levin, at *15.

2. Independent of the Constitutional Violation, Suppression Is Warranted By Intentional or Prejudicial Violations of Rule 41.

A non-constitutional violation of Rule 41 still warrants suppression when either 1) the defendant “suffered prejudice,” or 2) “the government intentionally violated the rule.” *United States v. Hurwitz*, 459 F.3d 463, 473 n.6 (4th Cir. 2006); *Simons*, 206 F.3d at 403.

Prejudice can be established by “a showing that the search would not have taken place the same way” if Rule 41 had been followed. *United States v. Graham*, 796 F.3d 332, 373 (4th Cir.), *reh'g en banc granted*, 624 F. App’x 75 (4th Cir. 2015). “Here, had Rule 41(b) been

³ In *United States v. Glover*, the D.C. Circuit was presented with a warrant that violated the territorial provisions of Rule 41(b) and the relevant statute. 736 F.3d 509, 515 (D.C. Cir. 2013). The court rejected the government’s argument that this did not amount to a “jurisdictional flaw in the warrant”: “[W]e do not see how a blatant disregard of a district judge’s jurisdictional limitation can be regarded as only ‘technical.’” *Id.* The *Glover* court reversed for the district court’s failure to suppress.

followed, *the magistrate judge would not have issued the NIT Warrant*, and therefore the search conducted pursuant to that Warrant might not have occurred.” *Levin*, at *9 (emphasis added).

Because the Rule 41 deficiency relates to the very issuance of the warrant, it makes no difference that Mr. McLamb’s computer happened to be located within the Eastern District of Virginia when the government hacked it. The NIT Warrant was void *ab initio*. Had the magistrate judge not acted beyond her statutory authority, the NIT Warrant would never have been issued.

The counter-factual is demonstrated by magistrate judge’s opinion denying a government application for a warrant to employ NIT malware in a different investigation. In *In re Warrant*, the government sought authority to conduct a search—or in the words of the court “to hack a computer”—by “surreptitiously installing software designed ... to extract certain stored electronic records.” 958 F. Supp. 2d at 755. As in this case, the government sought to install its malware on “an unknown computer *at an unknown location*.” *Id.* (emphasis added). Like the government did here in the NIT Warrant application, Ex. B, the government admitted in *In re Warrant* that “the current location of the Target Computer is unknown.” *Id.* at 756. On that basis, the magistrate deemed that the government was asking him to issue a search warrant that exceeded “the territorial limits on a magistrate judge’s authority to issue a warrant.” *Id.* The magistrate judge here should have done the same. And if she had, the NIT Warrant would not have issued at all.

Prejudice exists when the “the Government would not have obtained [the warrant] had Rule 41(b)(1) been followed.” *Krueger*, 809 F.3d at 1116. Here, not only did *this particular* NIT Warrant not comply with Rule 41, the magistrate *could not* have issued an NIT warrant that

followed Rule 41. The whole point of the NIT Warrant was to search computers *to determine their location*. Before deploying the NIT, the government did not know where it was searching.

Thus, the only way to follow Rule 41 was not to issue an NIT warrant at all.

The FBI case agent in charge of the Playpen investigation has testified that the FBI could not have territorially limited the deployment of its NIT technology:

20	Q. So, Agent Alfin, when we started talking about the NIT we
21	talked about it in terms of a problem and a solution, the
22	problem being that, from the FBI's standpoint, you couldn't
23	identify the physical location or any identifying information
24	about the computer that was logging in to the Playpen site,
25	correct?

—D. Alfin - Direct—

1 A. Correct.

2 Q. And the NIT was a way of gathering that information.

3 A. Yes.

4 Q. So if the problem was that you didn't know the location
5 of the activating computer -- this may be obvious, but before
6 you search the user's computer with the NIT you don't know
7 where that computer is located, right?

8 A. Correct.

9 THE COURT: We went through that before, didn't we,
10 Counsel?

11 MR. GRINDROD: Okay.

12 BY MR. GRINDROD:

13 Q. So here in this case the NIT warrant authorized the FBI
14 to search any user or administrator who logged on to the
15 Playpen Web site, correct?

16 A. The warrant that was obtained here in the Eastern
17 District of Virginia did authorize us to utilize the NIT
18 against any user's computer after that user logged in to the
19 Web site with a user name and a password.

20 Q. If you could, imagine for me that the NIT warrant instead
21 said that you could only search the computer of a user if
22 that computer was located in the Eastern District of
23 Virginia.

24 A. I'm imagining it.

25 Q. Okay. With this technology that you used in this case

—D. Alfin - Cross—

1 you could not -- you couldn't do that, right?

2 A. As stated previously, the NIT was utilized because we did
3 not know the physical location of a computer before the NIT
4 was utilized.

Hrg. Tr., 31:20-33:4, *United States v. Matish*, Case No. 4:16cr16 (E.D. Va. May 19, 2016) (testimony of FBI Special Agent Daniel Alfin) (attached as Exhibit F).⁴

There was no way for the government to narrow the territorial scope of the NIT Warrant. When deploying the NIT, the government could not limit its searches to computers located within the Eastern District of Virginia. The FBI did not know the physical location of any computer it was searching until after the search was completed. Mr. McLamb was subject to the nationwide dragnet searches authorized by the NIT Warrant as much as someone in Massachusetts or Alaska. And the *ex post* determination that his computer happened to have been located in the Eastern District of Virginia cannot cure the *ex ante* jurisdictional flaw that infected the NIT Warrant at its inception. The NIT Warrant could not have issued without violating Rule 41(b), so the prejudice to Mr. McLamb is clear.

Moreover, the Rule 41 violation appears to have been deliberate. Rule 41(b)'s limitations are unambiguous. For that reason alone, courts have been skeptical of 'good faith' explanations for the government seeking warrants for searches that clearly violate Rule 41's limitations. *See, e.g., Glover*, 736 F.3d at 516 ("In any event, it is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'")

⁴ The defense requests that the Court accept the *Matish* transcripts, Ex. F, as evidence on Defendant's First and Second Motions to Suppress.

But here the government knew that search warrant applications seeking to deploy NIT malware against unknown computers in unknown locations had been denied because of Rule 41(b) concerns. *See In re Warrant*, 958 F. Supp. 2d at 757 (denying 2013 application for NIT warrant). The Department of Justice recognized the Rule 41 problem with NIT searches and DOJ actively lobbied the Rules Committee to change Rule 41 to allow such “remote searches.” In a September 18, 2013 letter to the Rules Committee proposing an amendment to Rule 41, the Department of Justice cited *In re Warrant*, noting that a “magistrate judge recently ruled that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of Rule 41.”⁵ Then—just months before applying for the NIT Warrant in this case, a DOJ memorandum offered examples of “remote search warrants” that could be issued under an expanded version of Rule 41(b): DOJ described a child pornography website located on the Tor network and suggested that expanding Rule 41 would allow the government to “identify the location of the individuals accessing the site...by sending a NIT to each computer used to log on to the website.”⁶

The clearest evidence of the deliberateness of the Rule 41 violation here, however, was the government’s misleading sworn statements in its application for the NIT Warrant. As noted above, the government knew that NITs present Rule 41 territoriality concerns that turn on the location of the items to be searched. In 2012—before the *In re Warrant* decision raised Rule 41

⁵ Letter from Mythili Raman, Acting Asst. Attorney Gen. to Hon. Reena Raggi, Chair, Advisory Committee on Crim. R., 2 (Sept. 18, 2013) (asking Committee “to update the provisions [of Rule 41] relating to the territorial limits for searches” to allow searches via “remote access”), available at <https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-pdf> (last visited Apr. 29, 2016).

⁶ Memo from David Bitkower, Deputy Asst. Attorney Gen. to Hon. Reena Raggi, Chair, Advisory Committee on Crim. R., 6-7 (Dec. 22, 2014), available at <https://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0040> (last visited Apr. 29, 2016).

concerns over NIT warrants—the government sought a NIT warrant in the District of Nebraska. When describing the location of the property to be searched, the FBI special agent in that case wrote that the property to be searched was “located in the District of Nebraska *and elsewhere*.” Search Warrant Aff., at 1, ECF No. 123-1, *United States v. Cottom*, Case No. 8:13-cr-108 (D. Neb. Apr. 16, 2014) (emphasis added) (attached as Exhibit G). This is because, indeed, the property to be searched pursuant to any NIT warrant can be located anywhere in the world.

The affiant for the Playpen NIT Warrant, FBI Special Agent Macfarlane, agreed under oath that the place to be searched pursuant to the NIT Warrant was the user’s home computer:

22	Q. So you agree that the activating computers were the place
23	to be searched, correct?
24	A. Yes.

Matish Hrg. Tr., 65:22-24. Special Agent Macfarlane testified that he knew at the time he applied for the NIT Warrant in this case that he was requesting authority to search computers located outside the Eastern District of Virginia:

19	Q. Now, you knew at the time that you requested this search
20	warrant that you were requesting authorities to search
21	computers wherever located, correct?
22	A. Yes, that's what's listed in the affidavit.
23	Q. And you knew that that meant that you would be requesting
24	authority to search computers that were located outside the
25	Eastern District of Virginia, correct?
1	A. Yes.

Id., at 62:19-63:1. Despite this knowledge, however, Agent Macfarlane’s sworn warrant application states on its face that the property to be searched was “*located in the Eastern District of Virginia*.” *See* Ex. B, 1 (emphasis added).

Special Agent Macfarlane admitted that he and the United States Attorney's Office together drafted the proposed warrant, including the assertion that the property to be searched pursuant to the NIT Warrant was located within the Eastern District of Virginia:

—D. McFarlane - Direct—

1 Q. You, in consultation with the United States Attorney's
2 Office, drafted this as a proposed warrant, correct?
3 A. Yes, this is a part of Exhibit 1A.
4 Q. And you filled in the part that says that the place to be
5 searched was the property located in the Eastern District of
6 Virginia, correct?
7 A. I personally didn't fill that in, but that was a part of
8 the affidavit that I was swearing out, yes.
9 Q. Part of the affidavit, so you were swearing out as part
10 of this that the property that you were searching, that you
11 were requesting authority to search pursuant to this warrant,
12 was located in the Eastern District of Virginia.
13 A. That's what this says, yes. My understanding of how this
14 warrant works could be explained, if you give me a moment.
15 Q. Well, it could be explained because, in truth, you were
16 requesting authority to search property that was located
17 anywhere in the world, right?
18 A. Yes, and that's what is stated in the affidavit as well
19 for the Judge to consider.

Id., at 64:1-19.

Special Agent Macfarlane went on to explain a legal theory pursuant to which the government claims that the NIT Warrant was authorized under Rule 41. But the contrast

between the 2012 FBI warrant application from Nebraska and the 2014 warrant application in this case is stark, and the following timeline is revealing:

- Nov. 15, 2012: FBI applies for NIT warrant in Nebraska and tells judge that property to be searched is located in the _____ District of Nebraska and elsewhere
- Apr. 22, 2013: Decision out of the Southern District of Texas holds that NIT warrant does not comply with the Rule 41 “territorial limits on a magistrate judge’s authority to issue a warrant.” *In re Warrant*, 958 F. Supp. 2d at 756.
- Sept. 18, 2013: Department of Justice asks Rules Committee “to update the provisions [of Rule 41] relating to the territorial limits for searches” to allow searches via “remote access.”⁷
- Sept. 2013 to Dec. 2014: Department of Justice lobbies for changes to Rule 41, citing the *In re Warrant* decision and identifying NIT deployments against child pornography sites as the basis for the requested change.
- Feb. 20, 2015: FBI and Department of Justice lawyers apply for NIT Warrant in Virginia and tell judge that property to be searched is located in the Eastern District of Virginia .

After an adverse ruling in 2013, the DOJ demonstrated through a series of letters and memoranda its understanding that Rule 41 does not presently authorize the kind of warrant the government sought here. It appears that the government decided to obtain a warrant that it knew was unauthorized under Rule 41(b)—in part by failing to flag for the Magistrate Judge the fact that it was seeking authorization to search property located outside the district—with the expectation that the government could fight out the suppression issue in the courts if it arose. This is exactly the sort of deliberate violation that the suppression remedy was designed to incentivize against.

⁷ Letter from Mythili Raman, *supra* at n.4

CONCLUSION

The NIT Warrant was issued without jurisdiction and thus was void *ab initio*. Accordingly, the resulting search was authorized by no warrant. Since warrantless searches are presumptively unreasonable, the evidence must be excluded.

Alternatively, the Court can avoid reaching the constitutional question and find either that Mr. McLamb was prejudiced by the clear violation of Rule 41 or that the government deliberately violated that rule when it applied for the NIT Warrant. In either case, suppression is likewise warranted.

Respectfully submitted,

ROBERT MCLAMB

By: _____/s/_____

Amanda C. Conner
VSB # 88317
Attorney for Robert McLamb
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0816
(757) 457-0880 (telefax)
amanda_conner@fd.org

Andrew W. Grindrod
VSB # 83943
Assistant Federal Public Defender
Attorney for Robert McLamb
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0800
(757) 457-0880 (telefax)
andrew_grindrod@fd.org

CERTIFICATE OF SERVICE

I certify that on the 29th day of July, 2016, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following:

Elizabeth M. Yusi
United States Attorney's Office - Norfolk
101 W Main St
Suite 8000
Norfolk, VA 23510
(757) 441-6331
Fax: (757) 441-6689
Email: elizabeth.yusi@usdoj.gov

By: _____/s/_____

Amanda C. Conner
VSB # 88317
Attorney for Robert McLamb
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0816
(757) 457-0880 (telefax)
amanda_conner@fd.org